UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,557	03/02/2004	Marufa Kaniz	H1248	3296

29393 7590 01/25/2008

ESCHWEILER & ASSOCIATES, LLC
NATIONAL CITY BANK BUILDING
629 EUCLID AVE., SUITE 1000
CLEVELAND, OH 44114

EXAMINER	
GEE, JASON KAI YIN	

ART UNIT	PAPER NUMBER
2134	

NOTIFICATION DATE	DELIVERY MODE
01/25/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing@eschweilerlaw.com

AK

Office Action Summary	Application No.	Applicant(s)	
	10/791,557	KANIZ ET AL.	
	Examiner	Art Unit	
	Jason K. Gee	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) *11-18* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *3/2/04 & 6/16/05*.
4) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communication: response to election/restriction filed on 10/18/2007 with acknowledgement of filing date of 03/03/2004.

2. Claims 1-10 are currently pending in this application. Claim 1 is an independent claims.

3. The IDS received 03/02/2007 and 06/16/2005 has been accepted.

4. This is a supplemental action in regard to the typographical error sent in the previous Office Action. This is discussed in the Interview summary that is attached.

Election/Restrictions

5. Applicant's election with traverse of Group II in the reply filed on 10/18/2007 is acknowledged. The traversal is on the ground(s) that the characterization of Group 2 is incorrect. This is not found persuasive because group II, as the applicants have stated, is directed to a single integrated circuited comprising two security processors for performing IPSec processing in parallel. Group 1 is not directed to such limitations. Group 1 does not limit the claims an IPSec processor or processing in parallel. The search for Group 1 is not required for Group II, and the search for group II is not required for group I. Searching the additional limitations for Group II is a burden to the Examiner.

The requirement is still deemed proper and is therefore made FINAL.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 9 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 9, the claim recites wherein the security system comprises more processors for encrypting and authenticating outgoing data than for decrypting incoming data. It is unclear what the applicants are trying to claim. The claims previously recite that there are two processors for encrypting and authenticating. Therefore, the claims must mean there is only one processor for decrypting. However, in light of the Applicant's specification, it seems that the two processor encrypting are the same processors for decrypting.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-5 rejected under 35 U.S.C. 103(a) as being obvious over Pham US Patent Application Publication 2003/0115447 (hereinafter Pham), in view of Fahrny et

al. US Patent Application Publication 20050169468 (hereinafter Fahrny), and further in view of Bolt et al. US patent Application Publication 2004/0243745 (hereinafter Bolt).

As per claim 1, Pham teaches a network interface system for interfacing a host system with a network to provide outgoing data from the host system to the network and to provide incoming data from the network to the host system, the network interface system comprising: a bus interface system adapted to be coupled with a host bus in the host system and transfer data between the network interface system and the host system (paragraphs 45 and 46, wherein bus interface are the iSCSI, and connects to the host systems and media controllers; and Figure 1, where a host connects with media controllers via the ISCSI); a media access control system adapted to be coupled with the network and to transfer data between the network interface system and the network (Figure 1, 7), paragraph 19, and throughout the reference; a memory system coupled with the bus interface system and the media access control system, the memory system being adapted to store incoming and outgoing data being transferred between the network and the host system (paragraph 19, 47, and throughout the reference); and a security system coupled with the memory system, the security system being adapted to selectively encrypt outgoing data and to selectively decrypt incoming data (paragraph 19, 47, 61, 78, 83, 108), wherein the security system comprises two processors for encrypting the outgoing data (paragraphs 78, 80, also Figure 3 with cryptoprocessors 72 and also Figure 7 with crypto engines 144), the two processors each being operable independent of one another to encrypt the outgoing data (Figure 7, in which they are not dependent on each other, also paragraph 61 and 62).

However, at the time of the invention, Pham does not explicitly teach wherein the security system is configured to send outgoing data packets alternately to one or the other processor for encryption. This is taught by Fahrny though, such as in paragraph 32, 33, and 38-46, and also in Figure 1. Fahrny teaches a variety of encryption engines, each specializing in a different type of encryption algorithm. When information needs to be encrypted, it goes to one of the engines, depending on which algorithm is needed.

However, at the time of the invention, Pham also does not explicitly teach the use of bus interfaces connected to a host bus. Pham teaches ISCSI, which is an example of a bus interface, which inherently connects to busses. ISCSI as a bus interface is shown throughout Bolt, such as in paragraphs 10, 21, and 34.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the Pham and Fahrny references. One of ordinary skill in the art would have been motivated to perform such an addition to provide an improved system for security processing, while providing upgrades to encryption/decryption. This is taught by Fahrny in paragraphs 6, 7, and 8. Further Pham and Fahrny are both directed to secure media encryption involving multiple processors in a network environment.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the Pham and Bolt references. Pham teaches parts connected to each other, but does not explicitly cite buses. However, Pham uses the term buses to show the connections throughout a computer system, including which a bus interface may be an iSCSI. These bus interfaces, as shown throughout Pham, connect systems

together to allow them to communicate. Utilizing these type of bus interfaces allow compression of data in parallel, as well as continuous streaming of data (paragraph 10).

As per claim 2, Pham teaches throughout the reference wherein the two processors are also operable to authenticate the outgoing data (paragraphs 10, 48, 49, and 78).

As per claim 3, Pham teaches wherein the two processors are functionally identical (paragraphs 76 and 78, and also paragraphs 61, wherein processors are all the same).

As per claim 4, Pham does not explicitly teach wherein multiple buffers coupled to the multiple processors. However, this would have been obvious. Buffers are taught throughout Bolt, such as in paragraphs 37, 45, and 48, and they are used to temporarily store memory that is to be processed. At the time of the invention, it would have been obvious to one of ordinary skill in the art to implement multiple buffers for the multiple processors. As there are two processors both processing data in Pham, it would be obvious to attach a buffer to each processor, so as to manage the data flow to each processor. By managing the data flow to the processors, the system can operate more smoothly. Data buffers are known in the art to temporarily store information, and it would be obvious to store data/packets when this data is going to be subsequently used.

Claim 5 is rejected using the same basis of arguments used to reject claim 4 above. Although claim 4 discusses input buffers, output buffers are used in the same

way to temporarily store information that is going to be used subsequently, in order to allow the data to flow smoothly.

9. Claim 6 is rejected under 35 U.S.C. 103(a) as being obvious over Pham, Fahrny, and Bolt, as applied above, and further in view of Liu et al. US Patent Application Publication 2003/0169877 (hereinafter Liu)

As per claim 6, the Pham combination does not explicitly teach pipelines for ESP encryption , ESP authentication, and AH authentication. The Pham combination does teach that many encryption and authentication techniques may be implemented though (such as Pham 78 and also Fahrny paragraph 31). However, they do not teach the specific algorithms claimed. However, ESP encryption and authentication, as well as AH authentication, is taught throughout Liu, for example, in paragraphs 36, 40, 42 claim 1, etc.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include combine the Pham combination with Liu. One of ordinary skill in the art would have been motivated to perform such an addition to improve the efficiency of encryption and authentication in the IPSEC implementation in order to handle the obvious overhead on the network (paragraph 12).

10. Claim 7 is rejected under 35 U.S.C. 103(a) as being obvious over Pham, Fahrny, Bolt, and Liu as applied above, and further in view of Buer US Patent Application Publication 2004/0128553 (hereinafter Buer).

As per claim 7, the Pham combination teaches pipelining throughout Liu, but does not explicitly teach the HMAC-MD5-96 algorithm or the HMACH-SHA-1-96 algorithm. However, Buer teaches this, in paragraph 133.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the HMAC-MD5-96 or the HMAC-SHA-1-96 algorithm. Both these algorithms are well known in the art, and as the Pham combination is not restrictive on the algorithms used, it would have been obvious to substitute other algorithms for the ones already taught. Further, one of ordinary skill in the art would have been motivated to perform such an addition to improve packet processing techniques and to support secured data transmission over data networks (Buer paragraph 12)

11. Claim 8 is rejected under 35 U.S.C. 103(a) as being obvious over Pham, Fahrny, and Bolt, as applied above, and further in view of Sakai US Patent Application Publicaiton 2004/0093524 (hereinafter Sakai).

As per claim 8, the Pham combination teaches pipelining throughout Liu, but does not explicitly teach the DES-CBC, 3DES-CBC, and the AES-CBC encryption algorithms. However, this is taught by Sakai, such as in paragraphs 86, 87, and 144.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to include the DES-CBC, 3DES-CBC, and the AES-CBC algorithms. All these these algorithms are well known in the art, and as the Pham combination is not restrictive on the algorithms used, it would have been obvious to try and substitute other well known algorithms for the ones already taught.

12. Claim 9 is rejected under 35 U.S.C. 103(a) as being obvious over Pham, Fahrny, and Bolt.

As per claim 9, as best understood by the Examiner, Pham teaches wherein the security system further comprises a processor to selectively decrypt incoming data (paragraphs 47, 78, and claim 12). However, at the time of the invention, the Pham combination does not explicitly teach wherein the security system comprises more processors for encrypting and authenticating outgoing data than for decrypting incoming data. This would have been obvious though, and a design choice. It is common sense that more methods/steps would take more computing power. Authenticating and encrypting requires more processing power than just decrypting. To increase efficiency, it would have been obvious to one of ordinary skill in the art to allot more processors to processes that require more processing power. As decrypting is only one step, and authenticating and encrypting are two separate things, it would be obvious that authenticating and encrypting would require more processing power. Therefore, by providing more processors to encrypting and decrypting, the system would run more efficiently.

13. Claim 10 is rejected under 35 U.S.C. 103(a) as being obvious over Pham, Fahrny, and Bolt, as applied above, and further in view of Patt, Patel, Evers, Friendly, and Start's "One Billion Transistors, One Uniprocessor, One Chip" (hereinafter Patt).

As per claim 10, the Pham combination does not explicitly teach wherein the bus interface system, the media access control system, the memory system, and the security system, are included within a single integrated circuit. However, Patt discuses throughout the article that it is well know in the art and would be beneficial to put multiple computing devices onto one chip. For example, this is taught on page 51.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the teachings of Pham with Patt. One of ordinary skill in the art would have been motivated to perform such an addition to achieve higher performance by keeping latency to a minimum, by locating on the same chip as many as possible of the structures necessary to support a high-performance uniprocessor. Patt teaches this on page 51.

Conclusion

14. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-38383811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2100
01/08/2008

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER